2019

Cybersecurity Provisions and Trade Agreements

Chimene I. Keitner
keitnerc@uchastings.edu

Harry Clark

HARVARD
BUSINESS LAW
REVIEW

CYBERSECURITY AND TRADE AGREEMENTS: THE STATE OF THE ART

Chimène I. Keitner [†] *& Harry L. Clark* [††]

I. Introduction

Virtually without exception, conducting business across borders today means being connected to the Internet. The U.S.-Mexico-Canada Trade Agreement (USMCA), which is awaiting implementation by Congress, would become the first operative United States free trade agreement to include a chapter devoted to "digital trade."[1] The USMCA provisions on digital trade build on the electronic commerce chapter in the Trans-Pacific Partnership (TPP, now CPTPP)—a multilateral trade agreement that the Obama Administration negotiated, but the Trump Administration rejected.[2] As the United States continues to negotiate the conditions for its bilateral trade relationships, cybersecurity concerns are likely to feature in the discussions.

As a general matter, trade agreements seek to reduce barriers to cross-border trade. The prospect of negotiating a trade agreement can be used as a "carrot" in foreign relations, whereas punitive measures such as sanctions and tariffs are used as "sticks." Meanwhile, growing concerns about cybersecurity and the perceived risks posed by foreign technology and foreign control over data create pressures for more trade-restrictive arrangements. This essay examines provisions relating to digital trade and cybersecurity against the backdrop of these potentially competing interests. We begin by describing current efforts to address cybersecurity-related concerns in trade treaties, with a focus on the USMCA. Next, we address concerns at the intersection of cybersecurity and national security. Third, we identify an apparent trend towards company-specific

---

[†] Alfred & Hanna Fromm Professor of International Law, UC Hastings Law School; inaugural Orrick Scholar-in-Residence, Summer 2018.
[††] Partner & Chair of International Trade & Compliance Group, Orrick, Herrington & Sutcliffe LLP.
[1] Office of the U.S. Trade Representative, Agreement between the United States of America, the United Mexican States, and Canada, Nov. 30, 2018; *see* Roy Blunt, *USMCA: Where Things Stand*, SENATE REPUBLICAN POL'Y COMM. (Mar. 26, 2019), https://www.rpc.senate.gov/policy-papers/usmca-where-things-stand.
[2] *See, e.g.*, Anupam Chander, *The Coming North American Digital Trade Zone*, COUNCIL ON FOREIGN REL. (Oct. 8, 2018), https://www.cfr.org/blog/coming-north-american-digital-trade-zone (observing that "the TPP is dead, long live the TPP").

arrangements rather than global regimes. Finally, we offer an assessment of current efforts to use trade treaties to resolve cybersecurity and digital trade challenges.

II. Digital Trade and Cybersecurity Provisions in Regional Trade Agreements

Most industries rely on the movement of data to at least some degree.[3] Digital trade and cybersecurity provisions in trade agreements can thus have a widespread impact even beyond the obvious industries (internet platforms, e-commerce firms, online financial and payment services, computer services, and logistics firms).[4]

The idea of incorporating explicit cybersecurity provisions into international trade deals gained traction with the TPP, which was originally negotiated by the United States and eleven Pacific Rim countries (Australia, Canada, Japan, Malaysia, Mexico, Peru, Vietnam, Chile, Brunei, Singapore, and New Zealand). Russia and China have never been part of this framework. The TPP, which the United States ultimately abandoned, devotes a chapter to electronic commerce.[5] Article 14.16 (Cooperation on Cybersecurity Measures) affirms the importance of—but does not create concrete obligations for—"building the capabilities of their national entities responsible for computer security incident response" and "using existing collaboration mechanisms to cooperate to identify and mitigate malicious intrusions or dissemination of malicious code that affect the electronic networks" of the parties.[6]

Digital trade provisions of USMCA implement a "risk-based" approach to cybersecurity that may offer a path forward for at least the United States, Canada, and Mexico. This approach would rely on consensus-based standards and risk management best practices to identify and protect against cybersecurity risks and to detect, respond to, and recover from cybersecurity events. Perhaps not surprisingly, the digital trade provisions of USMCA echo the TPP's call to strengthen existing mechanisms for cooperating to identify and mitigate malicious intrusions that affect electronic networks. Unlike the TPP (which includes a greater number of parties, including several Asian countries), USMCA provisions contemplate use of those mechanisms to address cybersecurity incidents, as well as the sharing of information for awareness and best practices.

To date, regional agreements such as the CPTPP and USMCA have offered the clearest templates for reconciling digital trade facilitation with protections to consumers and core security interests.[7] Yet, complications can arise even in arrangements among friends. For example, when it comes to intelligence cooperation, some have suggested that aspects of intelligence-sharing among the "Five Eyes" could become more complicated if some members embrace a more open

---

[3] U.S.-Mexico-Canada Trade Agreement: Likely Impact on the U.S. Economy and on Specific Industry Sectors, Inv. No. TPA 105-003, USITC Pub. 4889, 171–72, n.412 (Apr. 2019) (Final).

[4] Along with provisions on digital trade, USMCA includes a chapter on telecommunications that governs access to networks, and a chapter on financial services that contains provisions on electronic payments.

[5] Office of the U.S. Trade Representative, Trans-Pacific Partnership Ch.14, Feb. 4, 2016; *see* Mark Wu, *Digital Trade-Related Provisions in Regional Trade Agreements: Existing Models and Lessons for the Multilateral Trade System*, INT'L CTR. FOR TRADE AND SUSTAINABLE DEV., at 6 (Nov. 2017), http://e15initiative.org/wp-content/uploads/2015/09/RTA-Exchange-Digital-Trade-Mark-Wu-Final.pdf.

[6] Office of the U.S. Trade Representative, *supra* note 5.

[7] *See* Wu, *supra* note 5, at 7 (describing the variety of e-commerce provisions in regional trade agreements).

approach towards Chinese-manufactured and developed equipment,[8] even if they commit to excluding such equipment from "sensitive" parts of their networks.[9]

The USMCA provides for increased consumer protection by requiring that each party adopt or maintain a legal framework that provides for the protection of the personal information of the users of digital trade. Chapter 19 specifies principles and guidelines that should underlie this framework: limitation on collection; choice; data quality; purpose specification; use limitation; security safeguards; transparency; individual participation; and accountability.[10] From the perspective of consumers, the most direct impact of Chapter 19 may be its provisions restricting the imposition of certain taxes, which will largely guarantee tax-free transfers of movies, e-books, and videos throughout the United States, Mexico and Canada. The agreement also establishes that platforms cannot be held liable for the actions of content producers, and it prohibits businesses from requiring that data be stored domestically.[11] Such anti-data-localization provisions also have implications for law enforcement, which increasingly confronts issues relating to cross-border access to digital evidence.[12] Public and private sector interests are increasingly interrelated because so much of our collective activity takes place on the same basic platforms.

III. National Security, International Trade and Cybersecurity

Just as trade and commerce have become increasingly digital, so too have elements of United States critical infrastructure.[13] The potential national security implications of policies that facilitate access to domestic networks and markets make this area susceptible to competing pressures.[14] For example, the Trump Administration and Congress view Chinese telecommunications as a profound threat to United States security, especially with respect to the design and deployment of 5G standards and systems.[15]

Although trade agreements have traditionally included some form of carve-out for measures deemed necessary to a country's "essential security," the pervasiveness of digital technology opens the door to expansive interpretations of this exception and what some have called

---

[8] Intel Brief, *Could Huawei Signal the End of the "Five Eyes"?*, CIPHER BRIEF (Mar. 28, 2019), https://www.thecipherbrief.com/column_article/could-huawei-signal-the-end-of-the-five-eyes.

[9] Michael Holden & Jack Stubbs, *Five Eyes Will Not Use Huawei in Sensitive Networks: Senior U.S. Official*, REUTERS (Apr. 24, 2019), https://www.reuters.com/article/us-britain-huawei-ncsc-usa/five-eyes-will-not-use-huawei-in-sensitive-networks-senior-us-official-idUSKCN1S01CZ.

[10] Office of the U.S. Trade Representative, United States-Mexico-Canada Agreement Ch. 19, Nov. 30, 2018.

[11] Jessica Vomiero, *Here's What You Need to Know About CUSMA and Digital Trade*, GLOBAL NEWS (Apr. 14, 2019), https://globalnews.ca/news/5166315/cusma-digital-trade-google/.

[12] Press Release, U.S. Department of Justice, Promoting Public Safety, Privacy and the Rule of Law Around the World (Apr. 2019), https://www.justice.gov/opa/press-release/file/1153446/download.

[13] *See generally* About CISA, CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY, https://www.cisa.gov/about-cisa.

[14] *See* Kathleen Claussen, *Beyond Norms: Using International Economic Tools to Deter Malicious State-Sponsored Cyber Activities*, 32 TEMPLE INT'L & COMP. L.J. 113, 115 (2018) (Kathleen Claussen has explored the potential for international economic tools to address certain malicious cyber activities by other states.).

[15] *See, e.g.*, Ellen Nakashima, *Current, Former Pentagon Leaders Sound Alarm on Chinese Technology in 5G Networks*, WASH. POST (Apr. 3, 2019), https://www.washingtonpost.com/world/national-security/current-former-pentagon-leaders-sound-alarm-on-chinese-technology-in-5g-networks/2019/04/02/d74f2bfe-54ab-11e9-9136-f8e636f1f6df_story.html?utm_term=.43d18a2c27dc.

a new "digital protectionism."[16] Even good-faith measures designed to reduce the risk of importing devices programmed with, or vulnerable to, malicious code can create barriers to trade. Moreover, just as the United States' introduction of self-judging essential security interest clauses into its bilateral investment agreements led to an overall increase in the inclusion of this type of clause in bilateral investment treaties around the world, [17] cybersecurity provisions in United States trade agreements could have a similar demonstration effect. Although some have argued that the existing World Trade Organization (WTO) framework governing Technical Barriers to Trade (TBT) could be used to assess national cybersecurity measures ostensibly adopted for legitimate purposes,[18] the current trend suggests that more specific negotiated language will ultimately supply the rules for digital trade and related flows of technology and data, as illustrated above.

Concerns about national security threats from international trade have grown sharply under the Trump Administration and reached a fever pitch over issues relating to China's leading telecommunication company's violation of sanctions related to Iran and North Korea.[19] The flashpoint has been the United States government's treatment of China's leading telecommunications company, Huawei, and China's second largest telecommunications equipment maker, ZTE. In April 2018, the United States Commerce Department generally banned supply to ZTE of items that were made in or have other connections to the United States after United States authorities found that ZTE violated United States' sanctions prohibiting most sales of such items to North Korea and Iran. The Trump Administration brokered a deal to levy a $1 billion fine on the company in lieu of the ban (in addition to earlier criminal and civil penalties).[20] Many members of Congress expressed disappointment in the lifting of the ZTE sanctions and threatened to reverse the action legislatively. While there was no legislative reversal, Congress included in the National Defense Authorization Act (NDAA) for fiscal year 2019 a variety of cybersecurity-related provisions aimed largely at ZTE, Huawei and other Chinese telecommunications companies.[21] For example, Section 889 of the NDAA instructs the executive branch not to procure telecommunications equipment or services from Huawei or ZTE.[22] (Huawei is challenging this provision in United States court.[23])

---

[16] Ziyang Fan & Anil Gupta, *The Dangers of Digital Protectionism*, HARV. BUS. REV. (Aug. 30, 2018), https://hbr.org/2018/08/the-dangers-of-digital-protectionism.

[17] Karl P. Sauvant & Mevelyn Ong, *The Rise of Self-Judging Essential Security Interest Clauses in International Investment Agreements*, COLUM. FDI PERS. No. 188, 1 (Dec. 5, 2016), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2881703&download=yes.

[18] *See* Alberto Oddenino, *Digital Standardization, Cybersecurity Issues and International Trade Law, Questions of International Law*, 51 QUESTIONS OF INT'L L. 31, 37 (May 31, 2018), http://www.qil-qdi.org/wp-content/uploads/2018/08/03_Data-Protection_-ODDENINO_FIN.pdf.

[19] *See, e.g.*, Charles Arthur, *Huawei, Sanctions and Software: Everything You Need to Know*, GUARDIAN (Dec. 8, 2018), https://www.theguardian.com/technology/2018/dec/08/huawei-sanctions-software-what-you-need-to-know.

[20] Will Knight, *ZTE May Have Been Saved, But Its Plight Could Strengthen China's Tech Ambitions*, MIT TECH. REV. (June 7, 2018), https://www.technologyreview.com/f/611382/zte-may-have-been-saved-but-its-plight-could-strengthen-chinas-tech-ambitions/.

[21] John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, 132 Stat. 1636 (2018).

[22] *Id.*

[23] *See* Quinta Jurecic, *Document: Huawei Lawsuit Against United States*, LAWFARE (Mar. 7, 2019), https://www.lawfareblog.com/document-huawei-lawsuit-against-united-states.

There was major escalation in 2019, when the Trump Administration sanctioned Huawei in response to alleged Iran embargo violations. In May 2019, the Commerce Department added Huawei and Huawei affiliates in twenty-six countries to the Export Administration Regulations' "Entity List."[24] Entity List rules generally forbid United States and non-United States companies from supplying to designated Huawei entities equipment, software and technology that originated in the United States, in whole or significant part, or that have certain other connections to the United States. These restrictions have substantially undermined international trade relating to telecommunications systems, particularly as they relate to the supply of semiconductor devices and designs. Chinese authorities have, in turn, threatened similar restraints on business with the United States.[25] While the United States has taken the most extreme approach, the United Kingdom and others have made findings that call the reliability of Huawei systems into question. These developments have occasioned major uncertainty and inefficiencies as countries struggle to move fully into the 5G era. The Huawei saga represents a particularly extreme example of the challenges governments and businesses will continue to face as trade issues and cybersecurity concerns increasingly intersect.

Given the specter of cybersecurity concerns connected to protecting national security and critical infrastructure, provisions regarding access to source code can provide a sticking point in digital trade negotiations. On the one hand, companies and countries require confidence that the code running on their systems has been checked for vulnerabilities and potentially malicious components. On the other hand, demands for access to source code can provide cover for state appropriation of proprietary technology. The European Commission has addressed this issue in part by promoting an open source software strategy and promulgating an open source software license (EUPL) to facilitate the sharing and reuse of software developed by public administrations.[26] In 2015, Vint Cerf and 260 experts urged the Federal Communications Commission (FCC) to require all manufacturers of Wi-Fi devices to make their source code "publicly available and regularly maintained," pointing to "[t]he recent Volkswagen scandal with uninspected computer code that cheated emissions testing" as proof that this is "a real concern."[27] Zeynep Tufekci of the University of North Carolina proposed in *The New York Times* in response to the Volkswagen debacle that we create "special commissions with full access to the code under regulatory supervision" to balance commercial interests and public safety in the Internet of Things.[28] Theodore Moran of Georgetown University authored a policy brief in 2013 advocating for the creation of a "multilateral nondiscriminatory procedure . . . for vetting IT goods and services—and patches and upgrades—from supply chains that originate anywhere in the world."[29]

---

[24] Addition of Entities to the Entity List, 84 Fed. Reg. 22961 (May 21, 2019) (to be codified at 15 C.F.R. § 744).

[25] *See, e.g.*, Alexandra Stevenson & Paul Mozur, *China Steps Up Trade War and Plans Blacklist of U.S. Firms*, N.Y. TIMES (May 31, 2019), https://www.nytimes.com/2019/05/31/business/china-list-us-huawei-retaliate.html.

[26] *See generally* Open Source Software Strategy, EUR. COMM'N, https://ec.europa.eu/info/departments/informatics/open-source-software-strategy_en (explaining the European Union's updated strategy for internal use of open source software).

[27] Darlene Storm, *Vint Cerf and 260 Experts Give FCC a Plan to Secure Wi-Fi Routers*, COMPUTERWORLD (Oct. 14, 2015), https://www.computerworld.com/article/2993112/vint-cerf-and-260-experts-give-fcc-a-plan-to-secure-wi-fi-routers.html.

[28] Zeynep Tufekci, *Volkswagen and the Era of Cheating Software*, N.Y. TIMES (Sept. 23, 2015), https://www.nytimes.com/2015/09/24/opinion/volkswagen-and-the-era-of-cheating-software.html?_r=0.

[29] Theodore H. Moran, *Dealing with Cybersecurity Threats Posed by Globalized Information Technology Suppliers*, PETERSON INST. FOR INT'L ECON., at 1 (May 2013), https://www.piie.com/sites/default/files/publications/pb/pb13-11.pdf (also praising Chinese company Huawei's existing security assurance program, which offers to place all source

In contrast to these code-sharing proposals, article 14.17 of the TPP (now CPTPP) precludes treaty parties from requiring "the transfer of, or access to, source code of software owned by a person of another [TPP] Party, as a condition for the import, distribution, sale or use of such software, or of products containing such software, in its territory."[30] This provision relates only to "mass-market software or products containing such software" and does not include software used for "critical infrastructure."[31] Annex 8-B on technical barriers to trade also provides that, with respect to information and communications technology products that use cryptography and are designed for commercial applications, "no Party shall impose or maintain a technical regulation or conformity assessment procedure that requires a manufacturer or supplier of the product, as a condition of the manufacture, sale, distribution, import or use of the product" to provide a private key or other encryption backdoor (although the agreement does not prevent a party's law enforcement authorities from requiring service providers that use encryption they control to provide unencrypted communications to law enforcement agencies "pursuant to that Party's legal procedures").[32]

The CPTPP therefore leaves it to businesses to negotiate source code verification provisions, if any, on a contract-by-contract basis, but it precludes the government of a state party to the agreement from mandating access to source code. Under this framework, providing access to source code for "mass-market software" cannot be a prerequisite for gaining access to a foreign market. Moreover, as indicated above, China, Russia, and the United States remain outside this framework.

Given the current geopolitical climate, the question remains whether an intermediate solution might be possible for source code inspection. IBM and Microsoft both experienced criticism in 2015 for agreeing to let the Chinese government review some of their proprietary code in a secure setting.[33] They, along with Intel, were among the most vocal opponents of China's plan to require foreign technology companies to provide the government with access to proprietary source code.[34] During the same period, Apple reportedly refused China's requests for its source code.[35] Meanwhile, companies including IBM, Hewlett-Packard, McAfee, Cisco, and the German company SAP agreed to use intermediary companies to allow the source code for their products to be inspected under requirements imposed by Russia's Federal Security Service.[36]

---

code in escrow to a trusted third party for verification; Moran is a member of Huawei's International Advisory Council).

[30] Office of the U.S. Trade Representative, *supra* note 5.

[31] *Id.*

[32] Office of the U.S. Trade Representative, Trans-Pacific Partnership Annex 8-B, Feb. 4, 2016.

[33] *See* Theodore H. Moran, *Should US Tech Companies Share Their "Source Code" with China?*, PETERSON INST. FOR INT'L ECON. (Oct. 28, 2015), https://www.piie.com/blogs/china-economic-watch/should-us-tech-companies-share-their-source-code-china.

[34] *See* Bogdan Popa, *Microsoft, Intel, Others Oppose China's Plans to Get Access to Source Code*, SOFTPEDIA NEWS (Dec. 5, 2016), https://news.softpedia.com/news/microsoft-intel-others-oppose-china-plans-to-get-access-to-source-code-510723.shtml.

[35] *See* Dustin Volz, *Apple Refused China Request for Source Code in Last Two Years: Lawyer*, REUTERS (Apr. 19, 2016), https://www.reuters.com/article/us-apple-encryption-idUSKCN0XG28Z.

[36] *See* Greg Price, *U.S. Tech Companies Give Russia Secretive Source Codes to Stay in Multibillion-Dollar Market*, NEWSWEEK (June 23, 2017), https://www.newsweek.com/russia-us-tech-source-code-628589.

In 2015, Stewart Baker expressed doubt that the prohibition on mandating access to source code in the TPP would have much impact given the carve-out for critical infrastructure, since "there's very little mass market software that doesn't run on computers involved in critical infrastructure."[37] In addition, even though the provisions on electronic commerce do not apply to government procurement, commercial software could well end up on products used by government employees (as Baker wrote, "I doubt US security agencies are comfortable letting Vietnam write apps that end up on the phones of their employees without the ability to inspect the source."[38]). This seems to leave no option but domestic development of software for critical infrastructure, or that might be used in government systems. However, a report by the United Kingdom Intelligence and Security Committee titled *Foreign Involvement in the Critical National Infrastructure; The implications for national security* observed that "[a]ny policy which seeks to block all Chinese companies from any future contracts relating to [Critical National Infrastructure] projects is not only impractical but, crucially, given the predominance of Chinese-manufactured and -developed equipment, is unlikely to result in the national security protection envisaged."[39] Current United States policy appears to be testing this proposition, as indicated above.

IV. Globalization, Regionalization, or Privatization?

As companies seek legal frameworks for conducting digital business on a global scale, factors continue to push in the direction of regionalized or localized rules. The specter has emerged of a division of the world between United States and Chinese cyber standards and communities of suppliers, particularly for 5G. The Trump Administration is reportedly contemplating requiring that 5G cellular technology deployed in the United States be made outside of China.[40] At the same time, United States sanctions are blocking Huawei's access to semiconductor devices and designs that are critical to 5G, such as re-programmable integrated circuits supplied by Xilinx and Intel.[41]

In the absence of a coordinated approach to cybersecurity and digital trade among governments, companies are embarking on their own initiatives. For example, Siemens AG and others have developed a Charter of Trust on cybersecurity, whose principles include promoting "multilateral collaborations in regulation and standardization to set a level playing field matching the global reach of [the] WTO" and "inclusion of rules for cybersecurity into Free Trade Agreements (FTAs)."[42] Microsoft has urged the need for a Digital Geneva Convention to curb

---

[37] Stewart Baker, *Cybersecurity and the TPP*, WASH. POST (Nov. 6, 2015), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/11/06/cybersecurity-and-the-tpp/.

[38] *Id.*

[39] INTELLIGENCE AND SECURITY COMMITTEE, FOREIGN INVOLVEMENT IN CRITICAL NATIONAL INFRASTRUCTURE; THE IMPLICATIONS FOR NATIONAL SECURITY 18 (June 2013), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/205680/ISC-Report-Foreign-Investment-in-the-Critical-National-Infrastructure.pdf.

[40] Leslie Jones, *Trump Administration Mulls Requiring 5G Equipment for Domestic Use to be Manufactured Outside of China: WSJ*, CNBC (June 23, 2019), https://www.cnbc.com/2019/06/23/us-considers-requiring-5g-equipment-for-domestic-be-made-outside-of-china-wsj.html.

[41] *See, e.g.*, John Kennedy, *Intel, Qualcomm, Xilinx and Broadcom Join Trump's Ban on Huawei*, SILICONREPUBLIC.COM (May 21, 2019), https://www.siliconrepublic.com/companies/huawei-intel-xilinx-qualcomm-broadcom-google-trump-ban.

[42] *Charter of Trust*, SIEMENS https://new.siemens.com/global/en/company/topic-areas/digitalization/cybersecurity.html (last visited Aug. 19, 2019).

states' malicious activities in cyberspace.[43] Ambassador Robert Holleyman, who led the creation of a new Digital Trade Working Group within USTR, has urged the United States to secure "21st Century rules for digital trade and data flows" in any new trade agreement with the European Union,[44] and former Commerce Department General Counsel Cam Kerry, responding to Holleyman, has called digital trade provisions "a gain lost by walking away from TTP and TTIP."[45] The ratification and implementation of the digital trade provisions of USMCA may provide some indication as to the feasibility of international commercial agreements in this area, while the ongoing trade war with China suggests that such solutions are not likely to achieve global reach.

In a better world, the United States and its trading partners would negotiate treaty arrangements that resolve with certainty and clarity the circumstances in which national governments can restrict digital trade for national security reasons. That would have been a tall order even in the halcyon post-World War II years in which the United States and its allies were far more prepared to cooperate on the intersection between international trade and national security. In current conditions, however, there seems to be little hope for multilateral treatment of a topic as charged with controversy as digital trade and national security. The USMCA, if it comes into effect, contains some promising language, but it does not offer a template for effective solutions on a broader scale.

The future, then, appears to lie largely with contractual arrangements among private parties that anticipate and account for national security-related disruption as best they can. Challenges such as United States sanctions against Huawei and ZTE are unlikely to dissipate anytime soon. As J. Benton Heath has cautioned, "[i]t is unclear whether our international economic systems have the legal tools, the capacity, or the legitimacy" to address the increasing entanglement between national security policy, including cybersecurity, and "ordinary" economic regulation.[46] The geographic fragmentation of digital supply chains is well underway.[47] Paradoxically, our increasing digital interconnectedness and interdependence could prompt the creation of regulatory barriers to cooperation that are as impermeable, if not more so, than physical ones.

---

[43] *Creating a Digital Geneva Convention*, MICROSOFT, https://news.microsoft.com/cloudforgood/policy/briefing-papers/trusted-cloud/creating-digital-geneva-convention.html (last visited Aug. 19, 2019).
[44] Robert Holleyman (@RHolleyman), TWITTER (Jul. 25, 2018, 2:09 PM), https://twitter.com/RHolleyman/status/1022227416171700224.
[45] Cam Kerry (@cam_kerry), TWITTER (Jul. 25, 2018, 2:33 PM), https://twitter.com/cam_kerry/status/1022233474139389952.
[46] J. Benton Heath, *National Security and Economic Globalization: Toward Collision or Reconciliation?*, 42 FORDHAM INT'L L.J. 1431, 1432 (2019), https://www.fordhamilj.org/volume-42-issue-5/2019/5/24/national-security-and-economic-globalization-toward-collision-or-reconciliation.
[47] *See* Debby Wu, *Trump Tumult Has Gadget Giants Splitting Along U.S.-China Lines*, BLOOMBERG (Aug. 14, 2019), https://www.bloomberg.com/news/articles/2019-08-14/the-world-s-gadget-makers-are-splitting-along-u-s-chinese-lines.